ADMINISTRACIÓN DE REDES

Imagen 1.

1. Conceptos básicos

Administrador o gestor de una red de datos

Persona encargada y por ende capacitada para la creación y soporte de infraestructuras de tecnología informática

El administrador de la Red propende por sus objetivos en los que se destacan:

Imagen 2.

- ✓ Mejorar la continuidad en la operación de la red con mecanismos adecuados de control y monitoreo, de resolución de problemas y de suministro de recursos.

- ✓ Hacer uso eficiente de la red y utilizar mejor los recursos, como por ejemplo, el ancho de banda.
- ✓ Hacer la red más segura, protegiéndola contra el acceso no autorizado, haciendo imposible que personas ajenas puedan entenderla información que circula en ella.
- ✓ Gestionar el mantenimiento de la red de modo que ocasione la menor interrupción posible en el servicio a los usuarios.

- **Administración de redes**

Se considera la administración de una red de datos tan compleja debido a que comprenden una mezcla de diversos servicios como voz, video, además de los datos; la interconexión de diferentes tipos de redes LAN, MAN y WAN; el uso de múltiples medios de comunicación como par trenzado, cable coaxial, fibra óptica, satelital, microondas; diversos protocolos de comunicación en los que se incluyen TCP/IP, SPX/IPX, SNA; el empleo de muchos sistemas operativos como DOS, Netware, Windows, UNIX y diversas arquitecturas de red tales como Ethernet, Token Ring, FDDI, entre otras.

2. Elementos de la administración de la red

Imagen 3

- **Objetos**: son los elementos de más bajo nivel y constituyen los aparatos administrados.
- **Agentes:** programa o conjunto de ellos, que coleccionan información de administración del sistema en un nodo o elemento de la red. El agente transmite información al administrador central acerca de:

- ✓ Notificación de Problemas
- ✓ Datos de diagnóstico
- ✓ Identificador del nodo
- ✓ Características del nodo

- **Administrador del sistema:** es un conjunto de programas ubicados en un punto central al cual se dirigen los mensajes que requieren acción o que contienen información solicitada por el administrador al programa agente.

3. Dimensiones en la administración de redes

La administración de redes es la suma total de todas las políticas, procedimientos que intervienen en la planeación, configuración, control, monitoreo de los elementos que conforman a una red con el fin de asegurar el eficiente y efectivo empleo de sus recursos. Lo cual se verá reflejado en la calidad de los servicios ofrecidos.

En este orden de ideas se definen 3 dimensiones en la administración de redes:

- **Dimensión Funcional:** Se refiere a la asignación de tareas de administración por medio de áreas funcionales.
- **Dimensión Temporal:** Se refiere a dividir el proceso de administración en diferentes fases cíclicas, incluyendo las fases de planeación, implementación y operación.
- **Dimensión del escenario:** Se refiere al resto de los escenarios adicionales al de administración de redes.

4. Administración de la configuración

- **Planeación y diseño de la red:** La meta de esta actividad es satisfacer los requerimientos inmediatos y futuros de la red, reflejarlos en su diseño hasta llegar a su implementación.

Imagen 4

El proceso de planeación y diseño de una red contempla varias etapas

- ✓ Reunir las necesidades de la red, las cuales pueden ser específicas o generales, tecnológicas (Multicast, Voz sobre IP, Calidad de servicio QoS), cuantitativas (cantidad de nodos en un edificio, cantidad de switches necesarios para cubrir la demanda de nodos).
- ✓ Diseñar la topología de la Red
- ✓ Determinar y seleccionar la infraestructura de red basada en los requerimientos técnicos y en la topología propuesta.
- ✓ Diseñar, en el caso de redes grandes, la distribución del tráfico mediante algún mecanismo de ruteo, estático ó dinámico.
- ✓ Si el diseño y equipo propuesto satisfacen las necesidades, se debe proceder a planear la implementación.

- **Selección de la infraestructura de la red:** Se realiza de acuerdo a las necesidades y la topología propuesta, por ejemplo si se propuso un diseño jerárquico, se deben seleccionar los equipos adecuados para las capas de acceso, distribución y núcleo. Además la infraestructura debe cumplir con la mayoría de las necesidades técnicas de la red. Lo más recomendable es hacer un plan de pruebas previo al cual deben ser sujetos todos los equipos que pretendan ser adquiridos.

- **Instalación de Hardware y administración del Software:** El objetivo de estas actividades son conseguir un manejo adecuado de los recursos de hardware y software dentro de la red.

Las tareas de instalación de hardware contemplan, tanto la agregación como la sustitución de equipamiento, y abarcan un dispositivo, como un switch o un ruteador, o solo una parte de los mismos, como una tarjeta de red, tarjeta procesadora, un módulo, etc.

Por otro lado, la administración de software, es la actividad responsable de la instalación, desinstalación y actualización de una aplicación, sistema operativo o funcionalidad en los dispositivos de la red. Además, de mantener un control sobre los programas que son creados para obtener información específica en los dispositivos.

Otra actividad importante es el respaldo frecuente de las configuraciones de los equipos de red ya que son un elemento importante que requiere un especial cuidado. Estos respaldos son de mucha utilidad cuando un equipo se daña y tiene que ser reemplazado ya que no es necesario realizar la configuración nuevamente.

- **Provisión:** Esta tarea tiene la función de asegurar la redundancia de los elementos de software y hardware más importantes de la red. Puede llevarse a cabo en diferentes niveles, a nivel de la red global o de un elemento particular de la red. Es la responsable de abastecer los recursos necesarios para que la red funcione, elementos físicos como conectores, cables, multiplexores, tarjetas, módulos, elementos de software como versiones de sistema operativo, parches y aplicaciones. Además de hacer recomendaciones para asegurar que los recursos, tanto de hardware como de software, siempre se encuentren disponibles ante cualquier eventualidad.

5. Administración de Rendimiento

Tiene como objetivo recolectar y analizar el tráfico que circula por la red para determinar su comportamiento en diversos aspectos, ya sea en un momento en particular (tiempo real) o en un intervalo de tiempo. Esto permitirá tomar las decisiones pertinentes de acuerdo al comportamiento encontrado. Se divide básicamente en dos etapas que son:

Imagen 5

- **Monitoreo**: consiste en observar y recolectar la información referente al comportamiento de la red en aspectos como los siguientes:

✓ Utilización de enlaces. Se refiere a las cantidades de ancho de banda utilizada por cada uno de los enlaces de área local (Ethernet, Fastethernet, GigabitEthernet, etc.), ya sea por elemento o de la red en su conjunto.

- ✓ Caracterización de tráfico. Es la tarea de detectar los diferentes tipos de tráfico que circulan por la red, con el fin de obtener datos sobre los servicios de red, como http, ftp, que son los más utilizados.
- ✓ Porcentaje de transmisión y recepción de información. Encontrar los elementos de la red que más solicitudes hacen y atienden, como servidores, estaciones de trabajo, dispositivos de interconexión, puertos y servicios.
- ✓ Utilización de procesamiento. Es importante conocer la cantidad de procesador que un servidor está consumiendo para atender una aplicación.

- **Análisis**: una vez recolectada la información mediante la actividad de monitoreo, es necesario interpretarla para determinar el comportamiento de la red y tomar decisiones adecuadas que ayuden a mejorar su desempeño. En el proceso de análisis se pueden detectar comportamientos relacionados a lo siguiente:

- ✓ Utilización elevada. Si se detecta que la utilización de un enlace es muy alta, se pueden tomar la decisión de incrementar su ancho de banda o de agregar otro enlace para balancear las cargas de tráfico.
- ✓ Tráfico inusual. El haber encontrado, mediante el monitoreo, el patrón de aplicaciones que circulan por la red, ayudará a poder detectar tráfico inusual o fuera del patrón, aportando elementos importantes en la resolución de problemas que afecten el rendimiento de la red.
- ✓ Elementos principales de la red. Un aspecto importante de conocer cuáles son los elementos que más reciben y transmiten, es el hecho de poder identificar los elementos a los cuales establecer un monitoreo más constante, debido a que seguramente son de importancia. Además, si se detecta un elemento que generalmente no se encuentra dentro del patrón de los equipos con más actividad, puede ayudar a la detección de posibles ataques a la seguridad de dicho equipo.
- ✓ Calidad de servicio. Otro aspecto, es la calidad de servicio o QoS, es decir, garantizar mediante ciertos mecanismos, las condiciones necesarias, como ancho de banda, retardo, a aplicaciones que requieren un trato especial, como son la voz sobre IP (VoIP), el video sobre IP mediante H.323, etc.
- ✓ Control de tráfico. El tráfico puede ser reenviado o ruteado por otro lado, cuando se detecte saturación por un enlace, o al detectar que se

encuentra fuera de servicio, esto se puede hacer de manera automática si es que se cuenta con enlaces redundantes.

6. Administración de Fallas

Imagen 6

Tiene como objetivo la detección y resolución oportuna de situaciones anormales en la red en las siguientes etapas:

- ✓ Una falla debe ser detectada y reportada de manera inmediata.
- ✓ Una vez que la falla ha sido notificada se debe determinar el origen de la misma para así considerar las decisiones a tomar.
- ✓ Las pruebas de diagnóstico son, algunas veces, la manera de localizar el origen de una falla.
- ✓ Una vez que el origen se ha detectado, se deben tomar las medidas correctivas para reestablecer la situación o minimizar el impacto de la falla.

Una falla puede ser notificada por el sistema de alarmas o por un usuario que reporta algún problema.

El proceso de la administración de fallas consiste de distintas fases tales como:

- ✓ **Monitoreo de alarmas**. Se realiza la notificación de la existencia de una falla y del lugar donde se ha generado. Esto se puede realizar con el auxilio de las herramientas basadas en el protocolo SNMP.
- ✓ **Localización de fallas**. Determinar el origen de una falla.
- ✓ **Pruebas de diagnóstico**. Diseñar y realizar pruebas que apoyen la localización de una falla.
- ✓ **Corrección de fallas.** Tomar las medidas necesarias para corregir el problema, una vez que el origen de la misma ha sido identificado.
- ✓ **Administración de reportes.** Registrar y dar seguimiento a todos los reportes generados por los usuarios o por el mismo administrador de la red.

7. Administración de la contabilidad

Es el proceso de recolección de información que permita describir el uso de los recursos que conforman la red. El primer paso es medir la utilización de todos los recursos para luego realizar un análisis que proporcione el patrón de comportamiento actual de uso de la red.

De aquí también se puede obtener información que ayude a planear un crecimiento o actualización de cada elemento que forma parte de la red, así como determinar si dicho uso es justo y adecuado.

8. Administración de la seguridad

Es ofrecer servicios de seguridad a cada uno de los elementos de la red así como a la red en su conjunto, creando estrategias para la prevención y detección de ataques, y la respuesta ante incidentes de seguridad.

Algunos aspectos a tener en cuenta en la administración de la seguridad son:

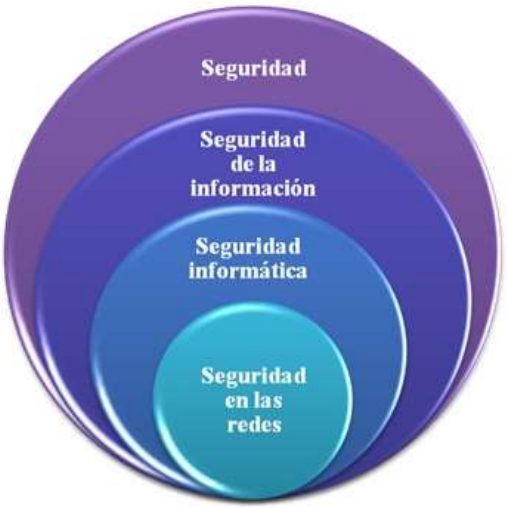

Imagen 7

- ✓ **Prevención de ataques**. El objetivo es mantener los recursos de red fuera del alcance de potenciales usuarios maliciosos. Una acción puede ser la implementación de alguna estrategia de control de acceso.
- ✓ **Detección de intrusos**. El objetivo es detectar el momento en que un ataque se está llevando a cabo. Hay diferentes maneras en la detección de ataques, tantas como la variedad de ataques del mismo. El objetivo de la detección de intrusos se puede lograr mediante un sistema de detección de intrusos que vigile y registre el tráfico que circula por la red apoyado en un esquema de notificaciones o alarmas que indiquen el momento en que se detecte una situación anormal en la red.
- ✓ **Respuesta a incidentes.** El objetivo es tomar las medidas necesarias para conocer las causas de un compromiso de seguridad en un sistema

que es parte de la red, cuando este ha sido detectado, además de tratar de eliminar dichas causas.

- ✓ **Políticas de seguridad**. La meta principal de las políticas de seguridad es establecer los requerimientos recomendados para proteger adecuadamente la infraestructura de cómputo y la información ahí contenida.
  Una política debe especificar los mecanismos por los cuales estos requerimientos deben cumplirse. El grupo encargado de ésta área debe desarrollar todas las políticas después de haber hecho un análisis profundo de las necesidades de seguridad.
  Entre otras, algunas políticas son:

  - cuentas de usuario
  - configuración de equipos de red
  - acceso remoto
  - Respaldo

Servicios de seguridad. Estos definen los objetivos específicos a ser implementados por medio de mecanismos de seguridad. La arquitectura de seguridad OSI, define que un servicio de seguridad es una característica que debe tener un sistema para satisfacer una política de seguridad.

La arquitectura de seguridad OSI identifica cinco clases de servicios de seguridad:

- Confidencialidad
- Autenticación
- Integridad
- Control de acceso
- No repudio

Mecanismos de seguridad. Se deben definir las herramientas necesarias para poder implementar los servicios de seguridad dictados por las políticas de seguridad.

Algunas herramientas comunes son:

- Herramientas de control de acceso, cortafuegos (firewall), TACACS o RADIUS
- mecanismos para acceso remoto como Secure Shell o IPSec,

- mecanismos de integridad como MD5, entre otras.

Todos estos elementos en su conjunto conforman el modelo de seguridad para una red de cómputo.

De las practicas rutinarias en la administración de redes como es la monitorización se puede mencionar que la técnica más primitiva es hacer pinging a los hosts críticos.

El pinging se basa en un datagrama de echo (eco), que es un tipo de datagrama que produce una réplica inmediata cuando llega al destino. La mayoría de las implementaciones TCP/IP incluyen un programa (generalmente llamado ping), que envía un eco a un host en concreto.

Si recibimos réplica, sabremos que host se encuentra activo, y que la red que los conecta funciona, en caso contrario, sabremos que hay algún error.

Técnicas más sofisticadas de monitorización necesitan conocer información estadística y del estado de varios dispositivos de la red. Para ello necesitará llevar la cuenta de varias clases de datagramas, así como de errores de varios tipos.

Este tipo de información será más detallada en los gateways, puesto que clasifican los datagramas según protocolo e incluso, él mismo responde a ciertos tipos de datagramas y es posible recopilar toda esta información en un punto de monitorización central.

Una forma más moderna para llevar a cabo la monitorización es a través de protocolos como el SNMP (Simple Network Management Protocol), que permite recoger información crítica de la red de una forma estandarizada.

Hay varias herramientas que visualizan un mapa de la red, donde los objetos cambian de color cuando cambian de estado, y hay cuadros que muestran estadísticas sobre los datagramas y otros objetos.

Una plataforma de monitorización es un conjunto de módulos software que ofrecen una serie de servicios en las que incorporan una interfaz gráfica de usuario que permite realizar las tareas más comunes.

Entre las plataformas de gestión existentes en el mercado tenemos:

- HP Open View Network Manager
- Sun SunNet Manager
- Aprisma Spectrum Site Manager Entre otros.

NNM (Network Node Manager) se compone de la plataforma SNMP y de una interfaz de usuario.

La interfaz de usuario se encarga de presentar:

La información de la red, Los eventos y alarmas Y tiene procesos que corren en segundo plano para monitorizar el estado y la configuración de los nodos, Mantener la base de datos con la información de la red.

REFERENCIAS

Alberto Caicedo, "Administración de redes de computadores, conceptos generales" recuperado de: https://www.academia.edu/11531163/ADMINISTRACI%C3%93N_DE_REDES_DE_COMPUTADORES_Conceptos_Generales

Imágenes:

Imagen 1, recuperada de:

http://administracion-de-redes-tec-iguala.blogspot.com.co/2016/05/41-elementos-de-la-seguridad.html

Imagen 2, recuperada de:

http://avanzasi.es/grupo-avanza-crea-el-cargo-de-gestor-de-red-de-proveedores/

Imagen 3, recuperada de:

http://elultimoynosbamos.blogspot.com.co/2011/02/administracion-de-redes.html

Imagen 4, recuperada de:

http://administracionderedeseq2.blogspot.com.co/

Imagen 5, recuperada de:

https://sites.google.com/site/informacionderedescuevas/optimizar-el-rendimiento-de-la-red

Imagen 6, recuperada de:

http://seguridadredes-angel.blogspot.com.co/2015/12/descripcion.html

Imagen 7, recuperada de:

http://redyseguridad.fi-p.unam.mx/proyectos/admonredes/PHP/capitulo6.html